

Industry

LEADING MEDIA COMPANY

EMPLOYEES - 2000+



CASE STUDY

LinkShadow and a leading media company in the region that has a wide range of media outreach including television, radio, print and digital platforms came together to work on streamlining the cybersecurity challenges around content security, protecting data and enhancing customer experience.

OBJECTIVES

- Ability to detect and respond to cyber threats quickly and effectively. What was lacking was advanced threat detection capabilities that can identify potential threats and vulnerabilities across the organization's networks, systems, and applications.
- To be able to protect sensitive information such as customer data, financial information, and intellectual property from cyber threats. This required strong data protection measures such as encryption, access controls, and monitoring.
- Insider threats can be particularly challenging for media organizations, where employees may have access to sensitive information and systems. There was need to implement monitoring and access controls to detect and prevent insider threats.
- Heavily reliant on third-party vendors for various services, which made them vulnerable to additional security risks. Therefore it was important to ensure that these vendors adhere to strict security standards and implement appropriate controls to mitigate the risks.
- Compliance to various regulations and standards related to cyber security. Meeting these requirements can be challenging and requires a comprehensive approach to cyber security analytics.



SOLUTION

LinkShadow intelligent NDR with UEBA helped address the cyber security challenges the customer faced. LinkShadow provided with a range of benefits that helped to mitigate the risks associated with cyber threats.

- Advanced threat detection capabilities helped identify potential threats and vulnerabilities across the organization's networks, systems, and applications. LinkShadow can monitor for suspicious behaviour and anomalies, detect, and alert on targeted attacks, and identify advanced threats like malware and ransomware.
- Helped monitor suspicious activity by employees and contractors, identify and prevent insider threats. LinkShadow provides visibility into user behavior, identify suspicious activity, and generate alerts in real-time.
- LinkShadow is monitoring third-party vendors and providing customer with visibility into their security posture. This can help identify and mitigate any security risks posed by third-party vendors.
- LinkShadow helped meet regulatory requirements and standards related to cyber security by providing a comprehensive approach to cyber security analytics. LinkShadow provided visibility into compliance with regulations and standards, generate compliance reports, and help to demonstrate compliance to auditors.

In summary, LinkShadow helped with enhanced threat detection, data protection, and visibility into security risks across its organization. By implementing an iNDR solution, customer managed to improve its cyber security analytics capabilities and mitigate the risks associated with cyber threats.

BENEFITS

Implementing LinkShadow intelligent NDR and UEBA solution significantly improved the security status of the customer. By providing enhanced threat detection and response capabilities, iNDR can help reduce the risk of cyber-attacks and protect SOC operations, customers, and reputation.

- Enhanced threat detection capabilities helped detect network-based threats, while UEBA helped identify unusual user behaviour that could be indicative of an attack.
- Enabled faster incident response by providing automated incident response capabilities that helped quickly remediate threats before they can cause damage or data loss. Also leveraged from the automated response capabilities to reduce the time to resolution and minimize the risk of damage or data loss.
- LinkShadow helped customer to adopt a more proactive approach to cyber security by identifying and remediating security risks before they could be exploited by attackers. iNDR can detect suspicious activity in real-time, while UEBA can identify anomalies in user behavior that could indicate a potential security risk.
- Empowered customer with improved visibility into their security posture, including the ability to monitor and analyze user behavior, network traffic, and system activity. The solution's advanced analytics capabilities helped with actionable intelligence to improve its security posture.